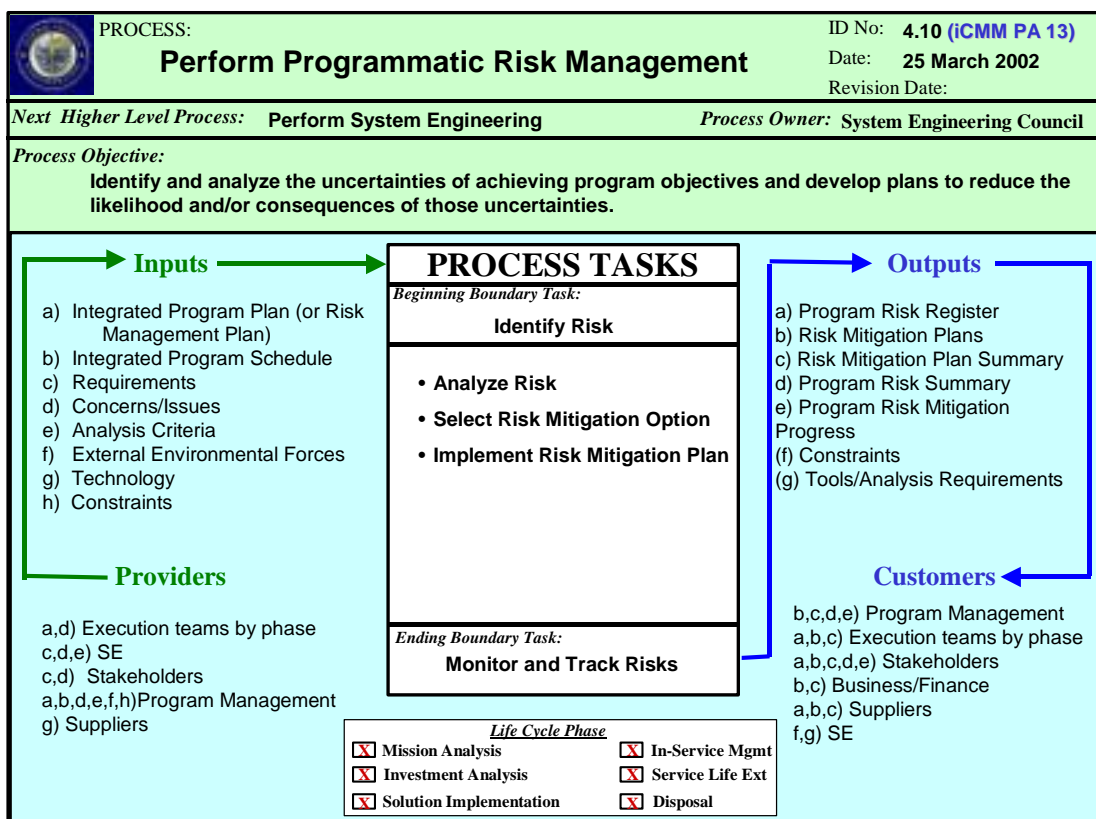1   **4.10 Programmatic Risk Management (*Satisfies iCMM process area 13 criteria*)**
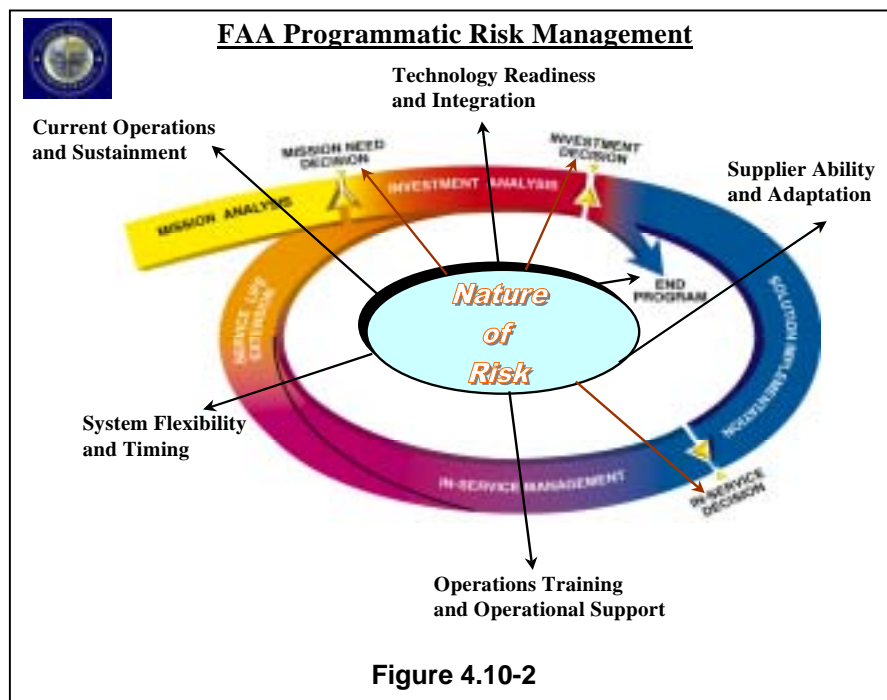
2   **4.10.1 Introduction**

3   The Perform Programmatic Risk Management process (Figure 4.1-10) provides an organized,
4   systematic decision-making process to effectively deal with uncertainty in accomplishing
5   program objectives. **Risk is defined as a future event or situation with a realistic (non-zero**
6   **nor 100 percent) likelihood/probability of occurring and an unfavorable**
7   **consequence/impact to the successful accomplishment of the well-defined program**
8   **goals if it occurs. Risk Management is an organized, systematic decision-support**
9   **process that identifies risks, assesses or analyzes risks, and effectively mitigates or**
10   **eliminates risks to achieve project objectives.** A risk creates *risk exposure* for a project
11   based on the combined effect of its likelihood and consequence. It is recommended that the
12   process be applied at all levels, from small projects to large programs, and be applied
13   continuously throughout the program's lifecycle looking at all aspects of the program (see Figure
14   4.10-2). The risks shall also be capable of being "rolled up" from a project or several projects to
15   a program. Risk roll-up involves a review of the consequences/impacts from a higher (program)
16   level. The risks to meeting the objectives or benefits of these projects or programs are typically
17   known as programmatic risks, though the source of these risks may be external to the program
18   itself. This process complies with the requirements of the integrated Capability Maturity Model
19   (iCMM) (Process Area 13). It also satisfies Electronic Industries Alliance (EIA) 632 requirement
20   24 and EIA 731 Focus Areas 2.5-2 through 2.5-8.

PROCESS: **Perform Programmatic Risk Management**	ID No: **4.10 (iCMM PA 13)**
	Date: **25 March 2002**
	Revision Date:
Next Higher Level Process: **Perform System Engineering**	*Process Owner:* **System Engineering Council**

Process Objective:
   Identify and analyze the uncertainties of achieving program objectives and develop plans to reduce the likelihood and/or consequences of those uncertainties.

Inputs

a) Integrated Program Plan (or Risk Management Plan)
b) Integrated Program Schedule
c) Requirements
d) Concerns/Issues
e) Analysis Criteria
f) External Environmental Forces
g) Technology
h) Constraints

Providers

a,d) Execution teams by phase
c,d,e) SE
c,d) Stakeholders
a,b,d,e,f,h)Program Management
g) Suppliers

PROCESS TASKS

Beginning Boundary Task:
   Identify Risk

• **Analyze Risk**

• **Select Risk Mitigation Option**

• **Implement Risk Mitigation Plan**

Ending Boundary Task:
   Monitor and Track Risks

Life Cycle Phase
[X] Mission Analysis   [X] In-Service Mgmt
[X] Investment Analysis   [X] Service Life Ext
[X] Solution Implementation [X] Disposal

Outputs

a) Program Risk Register
b) Risk Mitigation Plans
c) Risk Mitigation Plan Summary
d) Program Risk Summary
e) Program Risk Mitigation Progress
(f) Constraints
(g) Tools/Analysis Requirements

Customers

b,c,d,e) Program Management
a,b,c) Execution teams by phase
a,b,c,d,e) Stakeholders
b,c) Business/Finance
a,b,c) Suppliers
f,g) SE

4.1-10PBM

21

22   **Figure 4.10-1 Risk Management Process-Based Management Chart**

Figure 4.10-2

23 **4.10.1.1 Function of Programmatic Risk Management**

24 Programmatic risk management is a basic system engineering element of successful program
25 management (Figure 4.10-3). When properly executed, Risk Management engages all
26 disciplines and execution teams and is present in all program stages/phases. The functions
27 (Figure 4.10-4) of the process are to:

28 • Identify each risk to the program
29
30 • Analyze and assess the negative consequences/impact and the likelihood/probability of
31 the risk actually occurring and determine the risk realization date
32
33 • Develop specific approaches and plans to mitigate the risk
34
35 • Implement the risk-mitigation plan
36
37 • Monitor and track risk-mitigation effectiveness

38 Based on results from these functions, program management may then determine:

39 • The amount of schedule and budget reserves to be allocated and to what, based on
40 identified risks
41
42 • How to measure overall program performance with respect to each risk
43
44 • How much and what type of help is to be needed from other sources
45
46 • When to look at the process to see if the mitigation effort is working
47
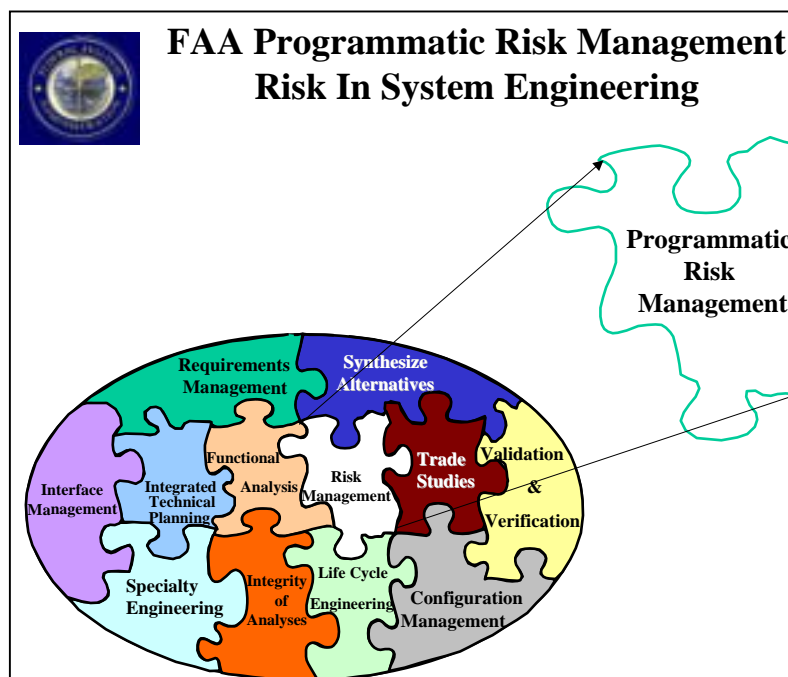48 • When to add mitigation efforts, costs, and milestones to integrated program schedule
49 and budget

FAA Programmatic Risk Management
Risk In System Engineering

Programmatic Risk Management

Requirements Management

Synthesize Alternatives

Interface Management

Integrated Technical Planning

Functional Analysis

Risk Management

Trade Studies

Validation & Verification

Specialty Engineering

Integrity of Analyses

Life Cycle Engineering

Configuration Management

50

Figure 4.10-3

FAA Programmatic Risk Management

Risk: A situation or circumstance which creates uncertainties about achieving program objectives.

Risk Management: An organized, systematic decision-support process that identifies risks, assesses or analyzes risks, and effectively mitigates or eliminates risks to achieve program objectives.

Programmatic Risk Management Plan 4.2.3.3

Identify Risk

Analyze Risk

Monitor and Track Risk

Select Risk Mitigation Option

Implement Risk Mitigation Plan

How Are Things Going?
Communicate Risks to all stakeholders
• Review mitigation actions for compliance to plan regularly
• Watch for new risks

What Can Go Wrong?
- Proposed changes
  - Staffing
  - Process
  - Design
  - Supplier
- Transition to operation checklists
- Test failures
- Failure to meet objectives
- Simulations
- Negative trends
- Issues list
- Interdependencies
- Safety
- Human Factors
- Integration
- ...And more

How Big Is the Risk?
- Categories
  Technical
  Schedule
  Cost
- Likelihood
- Consequences
- Identify the risk level from the 5x5 risk grid
- Determine risk resolution date

How Can You Reduce the Risk?
- *Avoid* by eliminating the risk cause and/or consequence
- *Transfer* the risk
- *Control* the cause likelihood and/or consequence
- *Assume* the risk level and continue on current plan
- *Research and Knowledge* of items that impact the risk
- Write mitigation plan

Does the Program include Mitigation ?
- Change budget to include Mitigation activity
- Change planning to include mitigation events
- Change schedule to include mitigation activity
- Communicate changes to stakeholders

Questions to Consider
• Does the risk statement describe a future event or situation?
• Is the source or cause of a risk based on factual evidence?
• Do others need to know about the risk?
• Is the risk mitigation plan adequate? Does the plan address the root cause of the risk?
• Are all stakeholders aware of the risk?

Figure 4.10-4

51 **4.10.1.2 Objectives of Programmatic Risk Management**

52 The fundamental objective of the Programmatic Risk Management process is to identify and
53 analyze uncertainties of achieving program objectives and develop plans to reduce the
54 likelihood and/or consequences of those uncertainties.

55 This process is applied to ensure that a program meets technical, schedule, and cost
56 commitments; delivers a product that satisfies all stakeholders' lifecycle needs; and provides the
57 expected benefit. Four lower-level objectives are established as part of meeting the overall
58 objective:

59 • Timely identification of risks (identifying a potential problem with sufficient leadtime so
60 the team may implement appropriate alternate plans)
61
62 • Consistent assessment of the level of risk across a program (providing a structured
63 decision-making framework for prioritizing resource application)
64
65 • Communication of risk-mitigation actions across the program/project (ensuring that all
66 elements of the program/project are aligned in resolving risks)
67
68 • Review of risk-mitigation action performance

69 **4.10.2 Process Description** *(Satisfies iCMM PA-14, BP13.04 criteria)*

70 Every participant in a program/project shares the responsibility of assessing and mitigating
71 risks. The process is a part of the overall program/project management and system engineering
72 process. This process shall be aligned with the individual products (hardware, services, and
73 software) that result from consistent functional analysis and requirements allocations, the
74 Integrated Program Plan (IPP), the integrated program schedule, the associated funding, and
75 the identified goals and benefits. The program is assessed as to risks associated with impacts
76 on program benefits, interdependent programs, or environments. For each product, risks are
77 evaluated against the acquisition baseline technical requirements, schedule, and cost leading to
78 the successful satisfaction of the program objectives. Risks are identified, assessed, and
79 appropriate risk-mitigation actions are established that comply with the program/project risk
80 management plan within the IPP (see Paragraph 4.2.2.2 in Integrated Technical Planning
81 (Section 4.2)). This plan is developed and tailored (when the technical nature of the program
82 demands tailoring) to satisfy the specific program/project needs (see Section 3.5.7). *(Satisfies*
83 *iCMM BP 13.01 criteria)*

84 Results from each assessment are a starting point for the risk-mitigation plan to support
85 program management decisions (technical, schedule, and cost). The products of this process
86 are also shared with stakeholders to achieve alignment/acceptance of the resource decisions.
87 All risks are examined at each program/project/event/item/peer review as defined in the risk
88 management plan. Updates reflect changes in risk resulting from planned mitigation activities or
89 other unplanned events. Risk progress is actively tracked. For each risk, a "risk realization
90 date" is established, marking the point in time when either the risk no longer exists or when the
91 program shall be modified to accommodate the negative consequences. The question to be
92 asked and answered is: "What happens on this date?" Risk is "rolled up" when it is taken from a
93 lower-level project to a higher-level program.

94 An essential element of the Programmatic Risk Management process from an organizational
95 point of view is the non-advocate concept. The purpose of a non-advocate is to provide an
96 impartial, objective assessment of the project team's results, especially with respect to the
97 assignment of risk levels. The input of a non-advocate is essential on those projects where two
98 or more of the project specialists disagree on the risk levels. A non-advocate would typically be,
99 but not be limited to, a program management person (above or at the same level of the
100 program/project manager), a stakeholder representative, and/or a person from another project
101 or program. The responsibility of a non-advocate is to examine and assess all aspects of the
102 program/project risk management process before each review. For small projects, one or two
103 non-advocates may be acceptable.   A non-advocate provides an assessment to
104 program/project managers for consideration and action.

105 **4.10.2.1 Overview**

106 The top-level process for Programmatic Risk Management is shown in Figure 4.10-1. The
107 process includes steps that result in the identification of potential risks, analysis and
108 assessment of risk, development of risk-mitigation plans, implementation of the Risk-Mitigation
109 Plan, and monitoring of risk status. The process is iterative and is used across the program
110 throughout the program's lifecycle, with the nature of the risks changing to coincide with the
111 lifecycle stage. Specific knowledge domains implement variants of this process to fit their
112 specific needs and environment. However, all domains effectively perform Risk Management
113 as shown in Figure 4.10-4.

114 **4.10.2.2 Inputs**

115 The inputs required to initiate Programmatic Risk Management include both program/project-
116 and product-related data as shown in Table 4.10-1. Many of these inputs are developed and
117 refined through the continuous, iterative use of other system engineering processes. Each item
118 in the table is to be evaluated for resultant program risk.

119   **Table 4.10-1. Inputs to Risk Management**

Input	Reference
Requirements Documents	4.3.3
Integrated Program Plan	4.2.1
System Engineering Management Plan (SEMP)	4.2.3.2
Risk Management Plan	4.2.2.2
Analysis Criteria	4.9.5.5
NAS Architecture	4.5.5
Trade Study Report	4.6.1.4
Design Analysis Report	4.8.4.3
Controlled Data and Reports	4.11.8
Contract	
Product Configuration Data	4.11.3
Acquisition Program Baseline (APB)	FAST
Acquisition Reviews	
Specialty Engineering Reports	4.8
Interfaces	
Test Plans and Reports	
Manufacturing/Production Information	
Resources/Budgets	

Input	Reference
External Uncertainties	
Technology	
Acquisition Strategy Paper	
Mission Need Statement	
Concept of Operations	
AMS Documents	
Technical Analysis	
Contractor Outputs	
Statement of Work	
Verification Results	4.12
Training Results	
Maintenance Results	
Lessons Learned	FAST
Operational Results	
Safety Assessments	
Security Assessments	
Human Factors Assessments	
Integrated Program Schedule	
Program Review Results	
System Safety Program Plan	4.8

120   **4.10.3 Risk Management Process Tasks**

121   The Programmatic Risk Management process is summarized in Figure 4.1-10. The major
122   process steps shown in Figure 4.10-4 are described in the remainder of this section.

123   **4.10.3.1 Task 1: Identify Risk** *(Satisfies iCMM BP 13.02 criteria*)

124   Risk identification is a systematic effort to uncover possible events or conditions that, if they
125   occur, may hinder achievement of program objectives. The process begins concurrently with
126   program or project planning and continues throughout the life of the program. While risk events
127   or conditions may have many different root causes (e.g., equipment interoperability
128   requirements, maintainability and supportability requirements, installation deadlines, contractual
129   arrangements), the identification process isolates those events or conditions that may affect
130   program technical performance, cost performance, or the program schedule. At the conclusion
131   of the identification phase of risk management, it is recommended that a program manager
132   have a list of (uncertain) events and conditions that may affect program cost, schedule, or
133   technical performance. Risk identification shall be performed during each stage of the program,
134   or whenever significant changes occur in plans or program status. Circumstances requiring risk
135   assessments include:

136   • Programmatic changes
137
138   • Unfavorable trends in Technical Performance Measures, predicted system performance,
139   schedules, and financial status
140
141   • Design/Program/Peer reviews
142
143   • Change proposals (including proposed changes in requirements)
144
145   • Occurrence of a major unforeseen event
146
147   • Newly identified risks
148
149   • Special assessments at the direction of Agency Management
150
151   • Changes or risks in interdependent programs
152
153   • Environment changes

154   As shown in Figure 4.10-5, participants in risk identification include all stakeholders, users,
155   suppliers, and appropriate members of execution teams. Teams consider all likely risk sources
156   in identifying potential risks to the program/project. Risk identification is based on the current
157   program/project goals supported by the associated technical, schedule, and cost requirements
158   and plans.

159   A programmatic risk has two aspects: (1) the likelihood/probability that an event will occur and
160   (2) an unfavorable consequence/impact if it occurs. It is recommended that the likelihood of a
161   risk occurring not be so low as to be negligible (i.e., probability essentially equal to zero) nor be
162   equal to 1, which typically indicates that it has, in fact, already been realized. A risk shall also
163   have a negative consequence/impact if realized. Positive consequences are not considered in
164   the FAA risk identification and analysis process; these are considered opportunities. Note that if

FAA Programmatic Risk Management
Risk Identification Flow

Man
Fun
Poli

- Operability
- Producibility
- Supportability
- Human Factors
- Security
- Safety
- Performance
Acquisition Strategy

Requirements

Cost

Schedule

Technical

Programmatic Risks

Figure 4.10-5
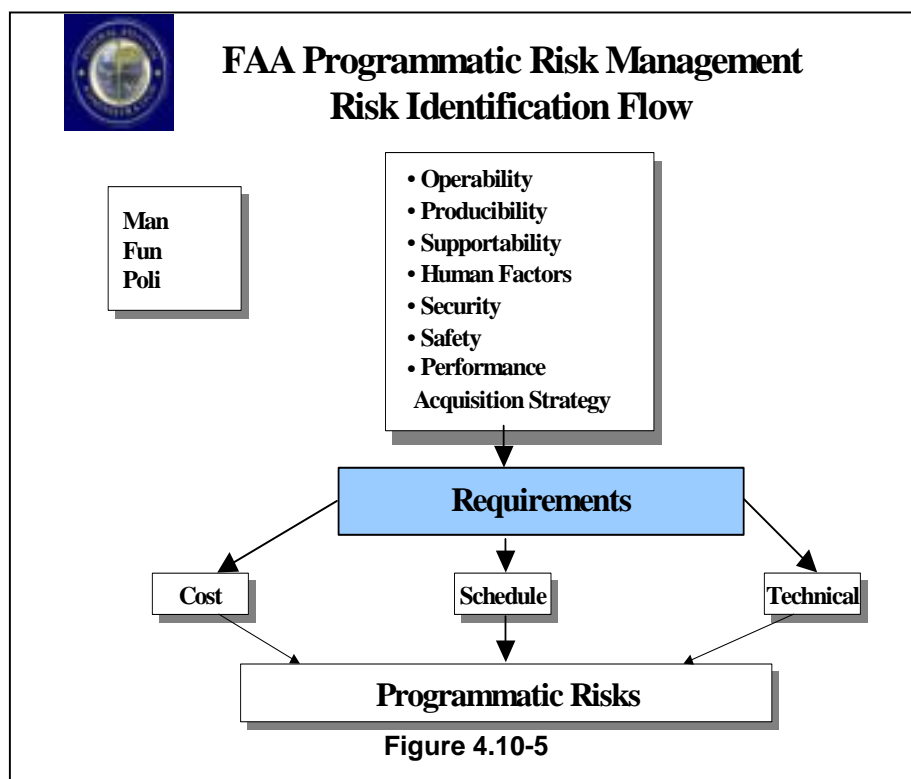
165   there is no uncertainty (i.e., the situation or circumstance is certain to occur or has already
166   occurred), there is no risk even though the item has an unfavorable consequence. It is
167   recommended that this situation be handled as a management issue, for which a corrective
168   action plan shall be generated and implemented. This essentially requires rebaselining the
169   program or possibly cancellation of the program if the negative consequences are too severe.

170   Each risk shall have a "risk realization date." This is a date when either the risk no longer exists
171   or when the program shall be modified to accommodate the negative consequences. This date
172   shall be documented when the risk is identified. The question to be asked and answered is:
173   "What happens on this date?" The negative consequence of the outcome of the event that
174   occurs on a given date is the basis for the risk.

175   **4.10.3.1.1 Potential Sources of Risk**

176   Risks originate from three basic areas—technical (or performance), schedule, and cost. A risk
177   identification flow is shown in Figure 4.10-5. Technical risk is based on the likelihood that the
178   program as planned will be unable to deliver a product to satisfy the technical requirements. As
179   such, well-documented, defined and quantified technical requirements are necessary to define a
180   technical risk. Most of the risks listed in Table 4.10-2 are technical risks. Schedule risk results
181   from the likelihood that the program actions may not be accomplished in the planned program
182   timing. A detailed program schedule identifying each accomplishment and the critical path is
183   necessary to develop schedule risks. Cost risk results from the likelihood that the program may
184   not accomplish planned tasks within the planned budget. A detailed budget, in which the cost of
185   each accomplishment is specified and any management reserve is known, is needed to
186   determine a cost risk. Potential loss of funding is not a programmatic risk in this risk process.
187   Within the FAA risk process, *cost* is the ultimate expenditure required for a resource and the
188   end product produced by that resource. **Budget** is the forecast of all costs planned for a given
189   project/program, and *funding* is the supply of money provided to accomplish a given
190   project/program. The risk source is based on the **root cause** of the risk and, as such, only a

191   single source will cause a risk. The source is technical, schedule, or cost in nature and not a
192   combination or all of these. This is not to be confused with the symptoms, which may manifest
193   themselves as some combination of performance (technical), benefit, cost, and/or schedule
194   impact.

195   A program's acquisition strategy generates risks in its own right. Development programs are
196   different in nature from those using commercial-off-the-shelf (COTS) solutions. Risks that need
197   to be considered in a COTS-based acquisition appear in Figure 4-10.6.

198   For each risk area, it is recommended that many sources be considered. For technical risk,
199   likely sources include technology maturity, complexity, dependency, stakeholder uncertainty,
200   requirements uncertainty, and testing/verification failure. Sources of schedule risks may include
201   incomplete identification of tasks, time-based schedule (as opposed to event-based schedule),
202   critical-path scheduling anomalies, competitive optimism, unrealistic requirements, and material
203   availability shortfalls. Cost risks may stem from an uncertain number of production units,
204   supplier optimism, additional complexity, change in economic conditions, competitive
205   environment, supplier viability, and lack of applicable historical data.

206   Table 4.10-2 provides the potential sources of risk that shall be considered in the process of
207   program risk assessment.

208

209   **Table 4.10-2. Potential Sources of Risk**

Potential Sources of Risk	
• Safety	• Test
• Security	• Verification
• Maintainability	• System Integration
• Reliability	• Staffing
• Supportability	• Tools
• Human Factors	• System Performance
• Availability	• Technology
• Decommissioning	• Planning
• Reducibility	• Transition
• Commonality	• Environments
• Training	• Interdependencies (both FAA and non-FAA)
• Operations	• Acquisition Strategy

210

COTS Considerations

Number	COTS Risk Factor (Characteristic)
01	COTS products can exhibit rapid and asynchronous changes.
02	COTS product obsolescence can affect systems in different ways.
03	COTS products are typically documented with proprietary data.
04	Low initial costs of COTS products can be offset by higher lifecycle costs.
05	Functionally equivalent COTS products/systems can have multiple configurations
06	Different COTS product vendors have different quality practices.
07	COTS products form, fit and function are sold "as is".
08	COTS products are developed to commercial standards.
09	COTS products typically have time-limited manufacturer support.
10	COTS product inter-operability can introduce information security susceptibility.

Figure 4.10-6

211

212 The knowledge domains of safety and security impose additional criteria or gates as part of their
213 identification process. In the case of safety, the process commences with an analysis, which
214 identifies potential hazards that are the basis for identifying safety related risks. Safety does not
215 identify a risk until a hazardous situation has been identified.
216
217 Information security engineering also utilizes a series of gates prior to identifying a risk. Security
218 is concerned about the existence of viable threats, which may exploit a system vulnerability to
219 cause harm. The combination of a viable threat coupled with a vulnerability in the system that is
220 capable of being exploited by the threat is necessary before the security community moves to
221 declare a (security) risk.
222
223 **4.10.3.1.2 Risk Identification Methods**

224 Risk identification begins at the lowest feasible level and normally includes inputs from all
225 stakeholders and suppliers. Anyone may identify a potential risk. It is recommended that
226 experts review programs to determine that risks related to their domain(s) have been completely
227 identified. It is also recommended that similar programs be reviewed for determined risks as
228 well as actual problems. The objective of this step is to produce as comprehensive a list as
229 possible of potential risks. This may be achieved using any combination of methods, such as
230 group discussions, interviews, trend/failure analysis, risk templates, lessons learned, trade
231 studies, Best Practices, metrics, and acquisition documentation. It is recommended that the

232   focus be on root causes and not on symptoms of a more basic problem. The problem shall be
233   defined at the lowest level (root cause) so that the mitigation plan actually addresses the
234   problem.

235   This process includes screening the list of risks for duplication and consolidation as appropriate.
236   Program Management errors are not risks and shall be corrected before the program moves
237   forward. It is recommended that this screening consider program-level ramifications and ensure
238   that program integration risks are adequately covered. A Risk Worksheet (Figure 4.10-7) may
239   be used to document newly identified potential risks.

240   **4.10.3.2 Task 2: Analyze and Assess Impacts of Risk** *(Satisfies iCMM BP 13.03 criteria)*

241   Risk analysis or risk assessment provides program insight into the significance of identified
242   risks. Risk analysis attempts to assess the likelihood of identified risks and the consequence to
243   the program if the risk event or condition occurs. The process also classifies each risk
244   according to the root cause of the risk event (cost, schedule, or technical performance).

245   Risk analysis assesses each component of an identified risk: (1) the likelihood of the risk
246   occurring, and (2) the consequence to the program if it occurs, as depicted in Figure 4.10-8.
247   The basic tool used for qualitative risk analysis is the risk template, which contains a set of
248   definitions to be used to evaluate the likelihood and consequence of a particular risk. The set of
249   templates that a program uses may change over time as new templates are added or existing
250   templates are changed, combined, or eliminated. The program may choose to use program-
251   unique templates (only if the technical elements of the program demand it), which are based on
252   and traceable to program or stakeholder requirements, provided supporting rationale is given.
253   However, modification of templates limits the ability to "roll-up" risks to a higher program level,
254   and, as such, a mechanism shall be developed to correlate risks developed through modified
255   templates to the risks developed with the standard FAA templates. The program/project is
256   responsible for the choice, coordination, and control of the templates used on the program.
257   These decisions are contained in the Risk Management Plan section of the SEMP (see
258   Paragraph 4.2.3.12 in Integrated Technical Planning (Section 4.2)).
259
260   The result of the risk analysis process is an assignment of a measure termed risk exposure to
261   each identified risk. Risk exposure is one quantitative figure of merit that represents the
262   combined effects of likelihood and consequence; it serves as an aid to program management in
263   ranking identified risks from most severe to least severe. At the conclusion of the risk analysis
264   process, it is recommended that program management have visibility into the range of possible
265   outcomes for the program (in terms of achieving objectives) if in fact an identified risk event or
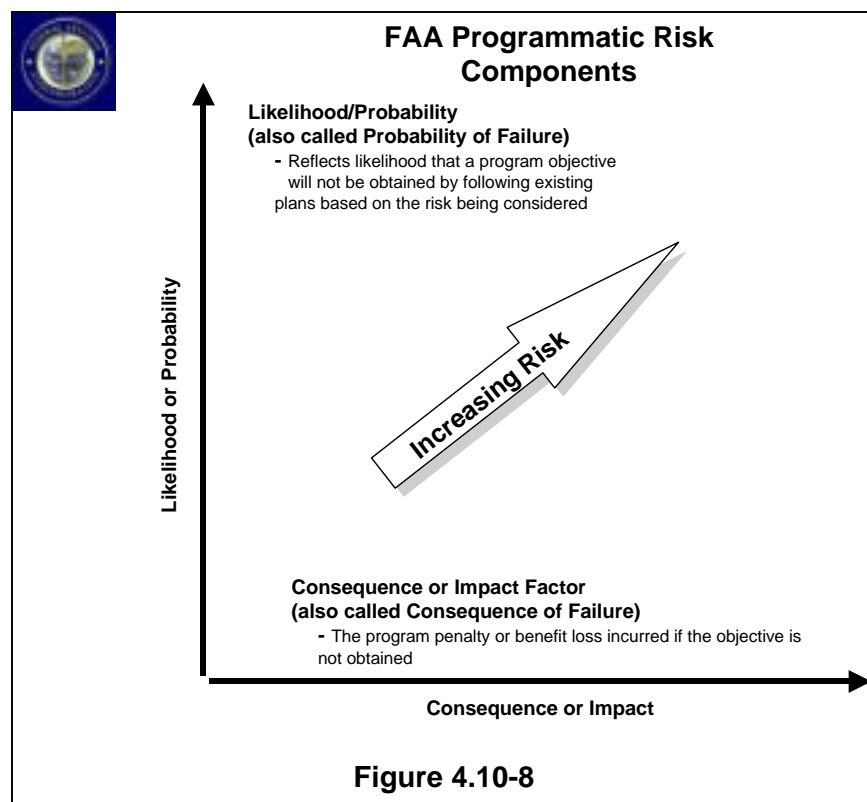266   condition occurs.
267

FAA Risk Worksheet

Program/Project Title_____ **Seq. #:** _____

Submitted by: _____ **Date:** _____

Risk:	Point of Contact

Source and Root Cause:

Risk Assessment			Rationale
o **Technical**	o **Schedule**	o **Cost**	
Likelihood	A B C D E		
Consequence	1 2 3 4 5		

Consequence Definition:

Risk Realization Date:

5	Mitigation Options	Description	New Risk Level if Implemented
☐	**Avoidance**		H M L
☐	**Transfer**		H M L
☐	**Control**		H M L
☐	**Assumption**		H M L
☐	**Research & Knowledge**		H M L

Figure 4.10-7

Figure 4.10-7

268

Figure 4.10-8

268
269 **4.10.3.2.1 Likelihood (Probability) Determination**

270 A likelihood (probability) template is developed that applies to the specific risk/program under
271 analysis. A new template is developed and documented if none of the existing program
272 templates are found to be applicable. This action shall be coordinated within the
273 program/project using the criteria of the Risk Management Plan. Correlation of the new
274 templates to the standard FAA templates in this manual shall be established. Figure 4.10-9
275 provides the FAA definitions of the risk likelihood levels.

276 **4.10.3.2.2 Consequence Determinations**

277 Another set of templates is used to evaluate consequence/impact to the program if the risk
278 materializes. Consequence templates are shown for three areas of program impact: technical
279 (Figure 4.10-10), schedule (Figure 4.10-11), and cost (Figure 4.10-12).   The choice of the
280 consequence template to be used to evaluate a given risk is determined by the nature of the
281 root cause of that risk. If the root cause is technical in nature, it is then recommended that the
282 technical consequences template be used. It shall be remembered that each of these results in
283 a programmatic risk, which threatens the benefits of a program and may also have
284 interdependency impacts. The symptoms of the risk may materialize in any combination of
285 program areas: technical (or performance), schedule, and/or cost. However, treating the
286 symptoms only wastes program resources and NOT directly deal with the source or root cause
287 of the risk.

288 All NAS programs are developed to provide benefit(s) to the system. Programmatic risk
289 ultimately reflects in impacts to benefit(s). All benefit losses are derived from losses in either
290 technical, schedule, or cost risks. This is a significant part of the risk consequence that shall be
291 defined. The cost/benefit analysis shall be reexamined as a result of cost and/or benefit
292 impacts to provide the information needed to make program decisions. As was the case with

293   likelihood templates, if none of the existing program consequence templates are found to be
294   applicable to a particular risk, new templates may be developed and documented. Correlation
295   of the new templates to the standard FAA templates in this manual shall be established.

FAA Programmatic Risk Likelihood Definitions

What is the likelihood the risk will happen?

1. Low: Your approach and processes will effectively avoid or mitigate this risk based on standard practices.

   The chance of a negative outcome based on existing plans is not likely. This likelihood level assessment should be based on evidence or previous experience and not on subjective confidence. This assessment level requires the approach and processes to be well understood and documented. Little or no management oversight will be required.

2. Minor: Your approach and processes have usually mitigated this type of risk with minimal oversight in similar cases.

   There is a low likelihood but reasonable probability that a negative outcome is possible. Present plans include adequate margins (technical, schedule, or cost) to handle typical problems. This assessment level requires the approach and processes to be well understood and documented. Limited management oversight will be required.

3. Moderate: Your approach and processes may mitigate this risk, but workarounds will be required.

   A negative outcome is likely, or the current approach and processes are only partially documented. Alternative plans or methods exist to achieve an acceptable outcome even if the risk is realized. Present plans include adequate margins (technical, schedule, or cost) to implement the workarounds or alternatives to overcome typical problems. Significant management oversight will be required.

4. Significant: Your approach and processes cannot mitigate this risk, but a different approach might.

   A negative outcome is highly likely to occur, or the current approach and processes are not documented. While alternative plans or methods are believed to exist to achieve an acceptable outcome, there are not adequate margins (technical, schedule, or cost) to implement the workarounds without impacting the program management reserves in performance, schedule, or cost. Significant management involvement is required.

5. High: Your approach and processes cannot mitigate this type of risk; no known processes or workarounds are available.

   A negative outcome is going to occur with near certainty. No alternative plans or methods have been documented. Alternatively, the risk item has yet to be evaluated adequately to be well understood, so there is a high level of uncertainty about the program success. Urgent management involvement is required.

Figure 4.10-9

296

FAA Technical Consequence Definitions

Given the risk becomes real, what would be the magnitude of the impact on system performance?

1. Low: Given that the risk is realized, there would be minimal impact.

   A successful outcome is not dependent on this issue; the technical performance goals will be met. There would be no impact on the success of the program.

2. Minor: Given that the risk is realized, there would be a minor performance shortfall but the same approach could be retained.

   The resulting technical performance would be below the goal but within acceptable limits. There would be no need to change the basic design, process, or approach. There would be no impact on the success of the program.

3. Moderate: Given that the risk is realized, there would be a moderate performance shortfall but workarounds would be available.

   The resulting technical performance would be below the goal. The basic design, process, or approach could be retained with only minor changes, and the overall system performance would still be acceptable as a result of workarounds such as the reallocation of functions or performance goals. There would be only a limited impact on the success of the program.

4. Significant: Given that the risk is realized, the performance would be unacceptable but workarounds would be available.

   The resulting technical performance would be unacceptably below the goal. The design, process, or approach would require a significant change to achieve an acceptable performance level. Additional workarounds such as the reallocation of functions or performance goals could also be required. The success of the program could be jeopardized.

5. High: Given that the risk is realized, the performance would be unacceptable with no known workarounds.

   The resulting technical performance would be unacceptably below the goal. There are no known alternatives or solutions. The success of the program would be in doubt.

Figure 4.10-10

296
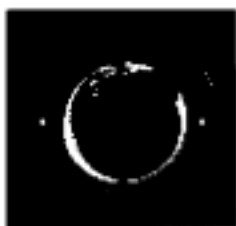
FAA Schedule Consequence Definitions

Given the risk becomes real, what would be the magnitude of the impact on the schedule?

1. Low: Given that the risk is realized, there would be minimal impact.

   The program schedule is not dependent on this issue. There would be no impact on the success of the program.

2. Minor: Given that the risk is realized, additional activities would be required to meet key dates.

   One or more key dates in the program schedule, but not critical path events, would be jeopardized; there are identified schedule workarounds that would be sufficient to mitigate the schedule impact. There would be no impact on the success of the program.

3. Moderate: Given that the risk is realized, there would be a minor schedule slip, and one or more need dates would be missed.

   One or more key need dates in the program schedule, but not critical path events, would be at least one month late; there are identified schedule workarounds that would be sufficient to keep the program critical path from being affected. There would be only a limited impact on the success of the program.

4. Significant: Given that the risk is realized, the program critical path would be affected.

   One or more events on the program critical path would be at least one month late. There are identified schedule workarounds that would be sufficient to meet major program milestones. The success of the program could be jeopardized.

5. High: Given that the risk is realized, a key program milestone cannot be achieved.

   Completion of a key program milestone would be late, and the success of the program would be in doubt. The slip requires a re-baseline of the program.

Figure 4.10-11

296

FAA Cost Consequence Definitions

Given the risk becomes real, what would be the magnitude of the impact on cost?

1. Low: Given that the risk is realized, there would be minimal cost impact.

   Program cost is not dependent on this issue. There would be no impact on the success of the program.

2. Minor: Given that the risk is realized, the total costs, operating cost or unit production cost would increase by = 1%.

   The program costs and/or the production unit cost would increase by = 1%. There would be no impact on the success of the program.

3. Moderate: Given that the risk is realized, there would be a minor increase in financial need. The program costs, operating cost or unit production cost could increase above 1% up to = 5%.

   The program costs and/or the production unit cost would increase above 1% to = 5%. There would be only a limited impact on the success of the program.

4. Significant: Given that the risk is realized, the total costs, operating cost or unit production cost would increase by above 5% to = 10%.

   The program costs and/or the production unit cost would increase above 5% to = 10%. The success of the program could be jeopardized.

5. High: Given that the risk is realized, the total costs, operating cost or unit production cost would increase by greater than 10%.

   The program costs and/or the production unit cost would increase by greater than 10%. The success of the program would be in doubt.

Figure 4.10-12

296

297   **4.10.3.2.3 Risk-Level Determination**

298   The likelihood and consequence are considered to be independent, but tied to the same event,
299   and are mapped into a risk grid to determine the individual risk level (e.g., high (red), medium
300   (yellow), or low (green)) as shown in Figure 4.10-13. This mapping facilitates the prioritization
301   and trend analyses of risks throughout the life of the program. Use of a "color code" for each
302   risk level supports effective communication of program health internally and externally.

FAA Programmatic Risk Management

Risk Grid

Figure 4.10-13
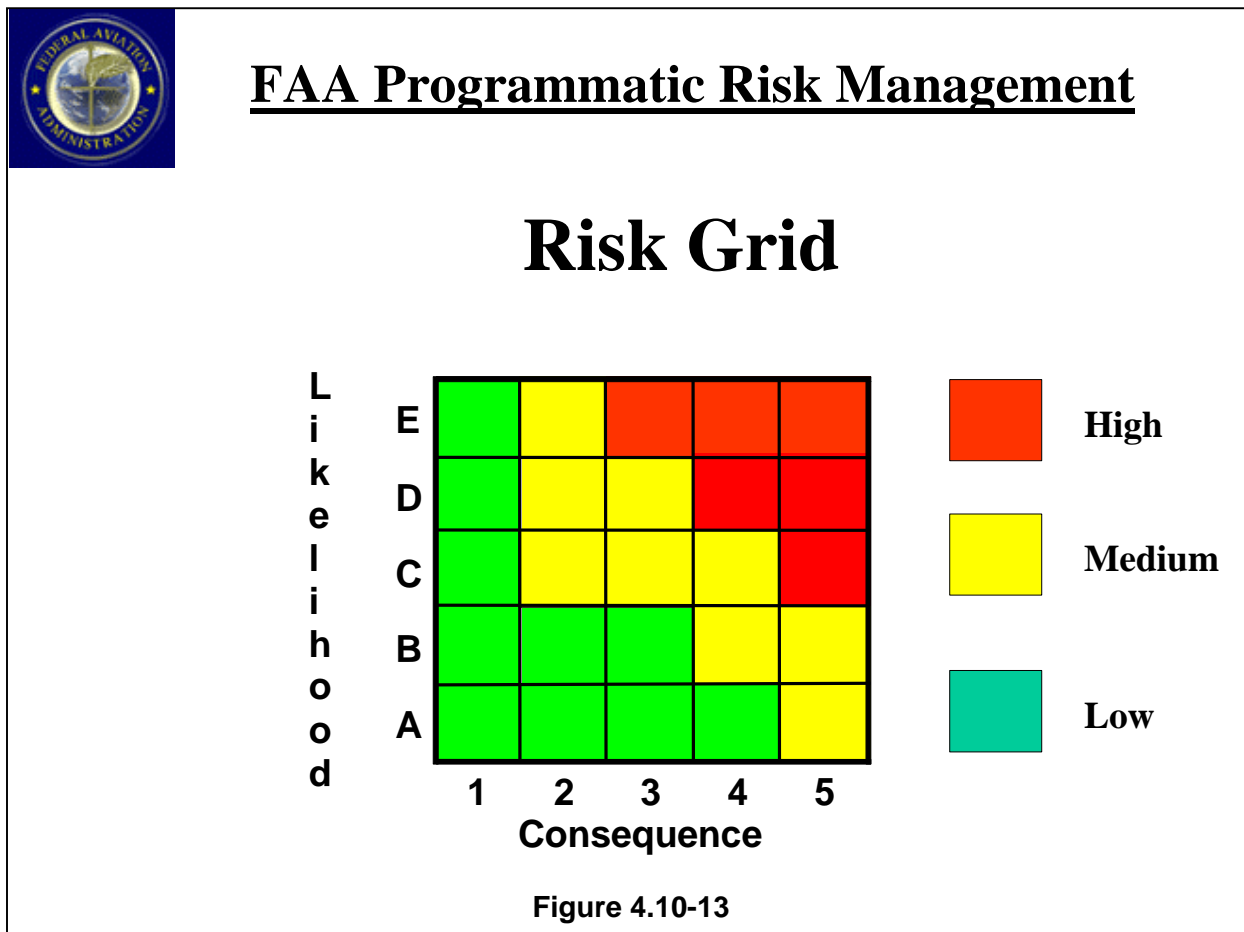
303   Risk-level definition high (red) is likely (a high probability) to cause significant disruption of
304   schedule, increase in cost, or degradation of performance. Concerted and continual emphasis
305   and coordination may not be sufficient to overcome major difficulties. Medium (yellow) may
306   cause some disruption of schedule, increase in cost, or degradation of performance. Special
307   emphasis and close coordination is probably sufficient to overcome difficulties. Low (green) has
308   little potential for disruption of schedule, increase in cost, or degradation of performance.
309   Normal emphasis and coordination is probably sufficient to overcome difficulties. The threshold
310   for differentiating between high, medium, and low may change from program to program, but not
311   for risk to risk, and it is recommended that it be determined early in the life of the program.

312   The color coding on this grid is also used to communicate management's threshold of risk
313   acceptability. For acquisition or development programs, this threshold is usually the line
314   between green and yellow. While development programs are focused on maturing a point

315

FAA Programmatic Risk Analysis

Consult non-advocates to support risk analysis

What is the Likelihood the risk will happen?

Level		Existing Infrastructure, Governance and Processes
E	Near Certainty	… cannot mitigate this type of risk; NO known processes or alternatives available. (>90% chance it WILL happen)
D	Highly Likely	… cannot mitigate this risk, but a different approach might. (>2/3 chance it WILL happen)
C	Likely	… may mitigate this risk, but alternative approach(es) may be required. (~50%chance it WILL happen)
B	Low Likelihood	… have usually mitigated this type of risk with minimal oversight in similar cases. (<1/3 chance it WILL happen)
A	Not Likely	… will effectively avoid or mitigate this risk based on standard practices. (<10% chance it WILL happen)

Likelihood

Always consider Interdependencies and benefits impacts

Given the risk is realized, what would be the magnitude of the impact?

Level	Technical	Schedule	Cost
1	Minimal Impact	Minimal Impact	Minimal Impact
2	Minor performance shortfall, same approach retained	Additional tasks required, able to meet key dates	Development or acquisition cost increase to≤1%
3	Moderate performance shortfall, ...alternatives available	Minor schedule slip, will miss need date without workaround	Development or acquisition cost increase >1% &≤5%
4	Unacceptable performance but alternatives available	Program critical path impact but workaround available	Development or acquisition cost increase >5% &≤10%
5	Unacceptable performance and NO alternatives exist	No known way to achieve program milestones	Development or acquisition cost increase >10%

Consequence

(Risk matrix: Likelihood E–A vertical, Consequence 1–5 horizontal, with High, Medium, Low regions)

316

Figure 4.10-14

317

318   solution for a requirements set, research is aimed at determining the feasibility of an approach
319   or technology. For research programs, the level of acceptability is typically defined as the
320   threshold between yellow and red because the success criteria of research do not require the
321   same degree of granularity as development. The degree of risk-level acceptance, and the
322   actions required to reduce a risk below that level shall be detailed in the Risk Management Plan.
323   Figure 4.10-14 is a summary of how the consequence and likelihood are consolidated to define
324   the risk level.

325   Various technical communities employ risk analysis techniques or methodologies specific to
326   their domain. They portray their conclusions and recommendations as grids similar to that
327   shown in Figure 4.10-14; but the scales vary from 3 x 3 to 10 x 10 with many variations in
328   between. It is recommended that the representation that a given specialty community (such as
329   Safety or Information Security) uses to draw conclusions be suited to its particular situation.
330   However, the criteria used and portrayal of a community's conclusions and/or recommendations
331   shall be consistent with the program view of risk. All risks need to be portrayed to management
332   on the same basis (see Section 4.10.3.5) to allow for effective decisions on the application of

333   risk-reduction resources. However, the basic conclusion(s) reached by the specialty community
334   shall be preserved in any translation into a common program reporting format.

335   The General Accounting Office (GAO) has defined a process to handle risk in a report issued in
336   2000 (Reference 16). It contains the same elements shown in the FAA Programmatic Risk
337   model with the exception of the track and control step. Figure 4.10-15 shows the correlation
338   between the two approaches and demonstrates how the GAO recommendations are satisfied
339   with the process described in the FAA SEM.

FAA Programmatic Risk Management

GAO Risk Assessment Process/Criteria

1. Identify Risk

Does the exposure relate to

- A program that has national significance?
- A management function that is key to performance and accountability?

No

Yes

Does the risk stem from

- An inherent vulnerability?
- A systemic problem?

No

Yes

IDENTIFY

Quantitative factors   Qualitative factors

Is the exposure to loss material in quantitative terms?

Is $1 billion or more at risk in areas such as:

- The value of major assets (e.g., loans receivables) being impaired?
- Revenue sources (e.g., taxes due) not being realized?
- Major agency assets (e.g., inventory, property) being lost, stolen, damaged, or wasted?

Could the risk be seriously detrimental to

Or

Could the risk result in

- Public health and safety?
- Service delivery?
- National security?
- National defense?
- Economic growth?
- Privacy or citizens' rights?
- Sensitive information?

- Significantly impaired service?
- Program failure?
- Significantly reduced effectiveness?
- Significantly reduced efficiency?
- Public injury or loss of life?
- Unreliable decision-making data?
- Reduced confidence in government?

2. Analyze Risk

Based on professional judgment, does the combination of qualitative and quantitative factors make the program or function high risk?

No

ASSESSMENT

Yes

3. Select Risk Mitigation Option

4. Implement Risk Mitigation Plan

Are corrective measures effective?

- Has the agency demonstrated a commitment to resolve the material control weakness?
- Has substantial progress been made to strengthen controls to address the risk?[1]
- Are corrective action plans appropriate?
- Will effective solutions be completed near term and get to the root causes of the problem?

Yes

No

Program or function is high risk

Program or function is not high risk

MITIGATE

GAO process requires examination of risk and the development of a mitigation effort. Shown is Figure 5 of GAO/OCG-00-12, Page 9. (August/2000).

Figure 4.10-15

341   **4.10.3.3 Task 3: Select Risk-Mitigation Option** *(Satisfies iCMM BP 13.05 criteria)*

342   The objective of risk-mitigation handling is to implement appropriate and cost-effective risk-
343   mitigation plans to mitigate or eliminate the risks. Appropriate risk-mitigation techniques are
344   selected and mitigation actions are developed, documented, and implemented. Risk-mitigation
345   handling (planning, implementation, and tracking) is the core of risk management. Risk-
346   mitigation implementation requires a conscious management decision to approve, fund,
347   schedule, and implement one or more risk-mitigation actions. Risk-mitigation plans and
348   mitigation actions are reviewed frequently at major reviews, program reviews, acquisition
349   reviews, and milestone reviews.

350   Risk-mitigation actions fall into one, or a combination, of the following strategies:

351   • Avoidance
352
353   • Transfer
354
355   • Control
356
357   • Assumption
358
359   • Research and Knowledge
360
361   "Avoidance" is a strategy to avert the potential of occurrence and/or consequence by selecting a
362   different approach or by not participating in the program. This technique may be pursued when
363   multiple designs or programmatic options are available. It is more likely used as the basis for a
364   "Go"/"No-Go" decision at the start of a program. Some examples are selection of state-of-the-
365   practice rather than state-of-the-art technologies and prequalification of suppliers. The
366   avoidance of risk is from the perspective of the overall program/project, which includes the
367   stakeholders, contractors, and execution groups. Thus, an avoidance strategy is one that
368   involves all of the major parties to the program/project and permits a program/project-wide
369   avoidance of the risk.

370   "Transfer" is a strategy to shift the risk to another area, such as another requirement, an
371   organization, a supplier, or a stakeholder. Examples include reallocating requirements,
372   securing supplier product warranties, and negotiating fixed-price contracts with suppliers. Note
373   that at the program level, the risk remains. The transfer of the risk is accomplished primarily to
374   optimize, in a sense, the overall program risk and to assign ownership to the party most capable
375   of reducing the risk. It is possible that the risk level may change as a result of the risk transfer.

376   "Control" is a strategy of developing options and alternatives and taking actions that lower or
377   eliminate the risk. Examples include new concepts, more analysis, redundant systems and/or
378   components, and alternate sources of production.

379   "Assumption" is simply accepting the likelihood/probability and the consequences/impacts
380   associated with a risk's occurrence. Assumption is usually limited to low risks. This is a
381   program/senior management option, not a program option. FAA practice is to develop
382   mitigation plans for all medium and high risks.

383   "Research and Knowledge" may mitigate risk through expanding research and experience.
384   Since risk arises from uncertainty and inexperience, it may be possible to effectively mitigate

385 risk simply by enlarging the knowledge pool, leading to reassessment that reduces the
386 likelihood of failure or provides insight into how to lessen the consequences.

387 At this point, several alternatives for mitigating the risk have been identified and analyzed for
388 selection of the preferred approach. Alternatives include detailed plans for mitigating the risk in
389 several small, sequential steps; alternative steps; or entirely new (nonbaselined) approaches to
390 accomplishing the program. Further, contingency plans are identifiable alternatives, which may
391 be implemented if a mitigation plan fails, and the risky event or conditions occur with more
392 serious consequences than anticipated. The mitigation steps are the major milestones of the
393 mitigation plan. Contingency plans need not be extremely detailed.

394 For instance, the risks associated with selecting a COTS-based acquisition approach (see
395 Figure 4.10-6) have known risk-mitigation strategies. These strategies need to be included in
396 the trade studies when comparing acquisition approaches. Because COTS has an inherent set
397 of risks that are market-driven, most of the risk-mitigation strategies fall into the "Control"
398 category in order to anticipate and reduce the risks to acceptable levels. More information on
399 COTS risks and mitigation strategies may be found in the FAA COTS Risk Mitigation Guide,
400 which is available at http://www.faa.gov/aua/resources/COTS.

401 Trade study techniques may be performed to help select the preferred risk-mitigation plan.
402 While the proper criteria and their weights for each analysis are dependent on the risks to be
403 mitigated, it is recommended that the following be included:

404 • Does the option mitigate the likelihood or consequence of the risk?
405
406 • Does the option fit within program scope?
407
408 • Is the option easy to implement?
409
410 • Are new risks avoided or introduced?
411
412 • What is the cost of mitigation?
413
414 • What is the schedule for mitigation?

415   The risk level is the first criterion used to determine the need for a risk-mitigation plan. Program
416   risks that fall into the medium or high categories require risk-mitigation plans. Risks that are
417   assessed as low typically do not require mitigation plans but may have certain aspects that
418   would be prudent to monitor. If this is the case, risk-mitigation plans may be formally or
419   informally implemented for these low-risk issues based on the specific Risk Management Plan
420   for a program.

421   It is essential that those responsible for plan implementation have a thorough understanding of
422   the risk to be mitigated. This may be accomplished with a good summary statement of the risk.
423   It is recommended that the statement include descriptions of the future event or condition, which
424   confirms trouble for the program; the root cause(s) of the event outcome or conditions; and the
425   specific effects to the program if the event or conditions occur with negative consequences. It is
426   recommended that the risk not be stated in terms of its mitigation plan.

427   It is recommended that the status also include a summary of risk-mitigation efforts that
428   references more detailed documentation. A Risk Mitigation Plan Summary (Figure 4.10-16) is
429   used to report the analysis and actions on an individual risk.

430   The risk-mitigation plan documents the specific steps to be implemented, the sequence in which
431   they are to be implemented, and the points in time at which they are to be implemented.
432   Developing a risk-mitigation plan includes assessing the expected outcome following
433   implementation. It is recommended that the same method initially used to assess the risk, such
434   as risk templates, be used to provide a forecast of the risk level after completion of each action
435   of the risk-mitigation plan. The expected impact of each mitigation event on risk level may be
436   projected using a format similar to that of Figure 4.10-17 (a "waterfall chart").

437

Risk ID No: __AND490-001__

Date: __04/15/3032__

Risk Mitigation Plan Summary
Sample

Page __1__ of __6__

Status: __Active__

Risk Title
Scan rate low

Program/Project __ASR-27__

Project Lead __Mr. Solo__

Description of Risk
The scan rate of the radar sail may fall below the allowable tolerance

Statement of Root Cause
Analytical projections of motor power available may have overestimated power resulting assumption that requirements could be satisfied.

Consequence if Realized **Low scan rate provides inadequate data rate to remote control function resulting in increased approach separation and increased delays**

Risk Type: **T** S C
Likelihood __D__
Consequence __3__
Comments:

Risk Resolution Date: 10/17/32

Place X in One Cell

Risk Mitigation

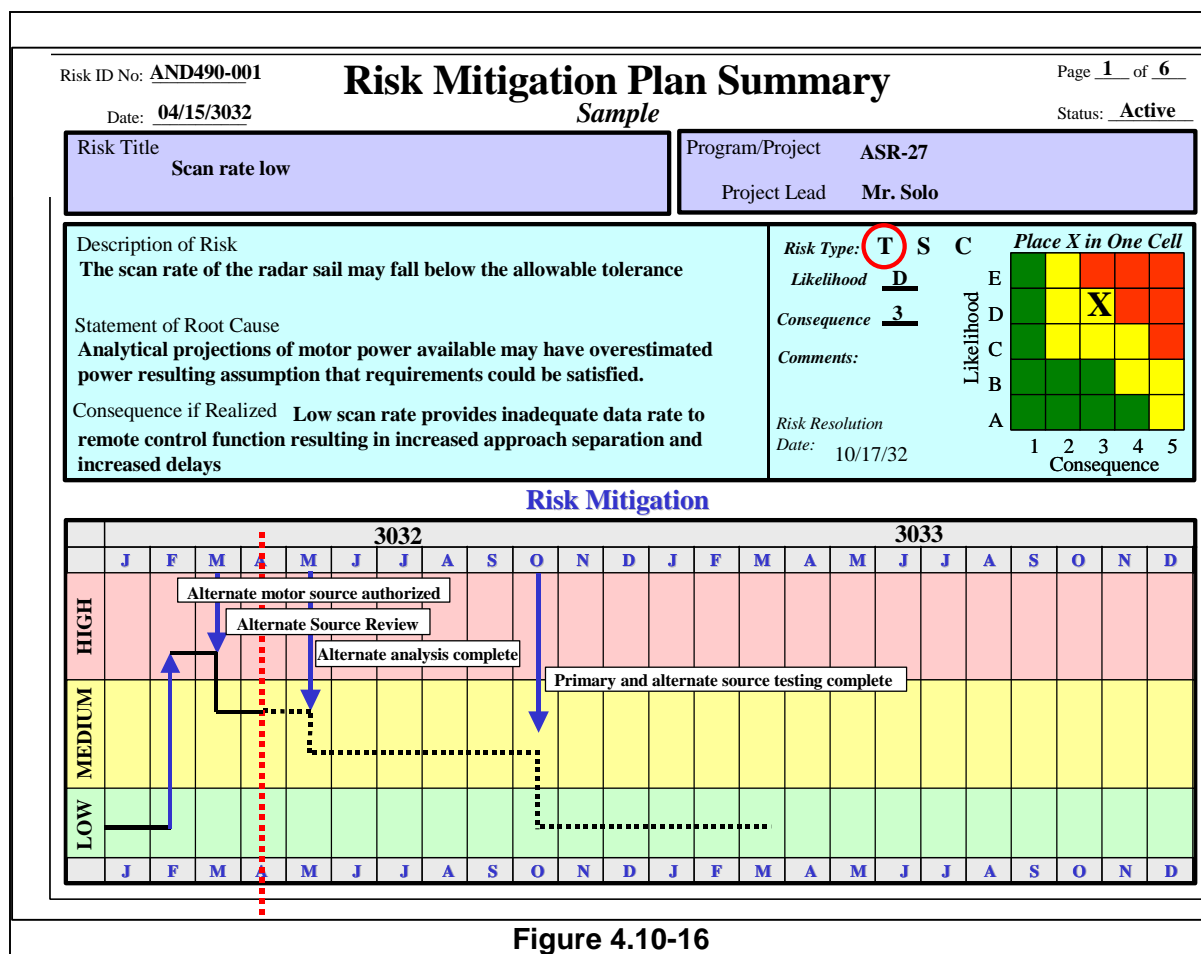**Figure 4.10-16**

437

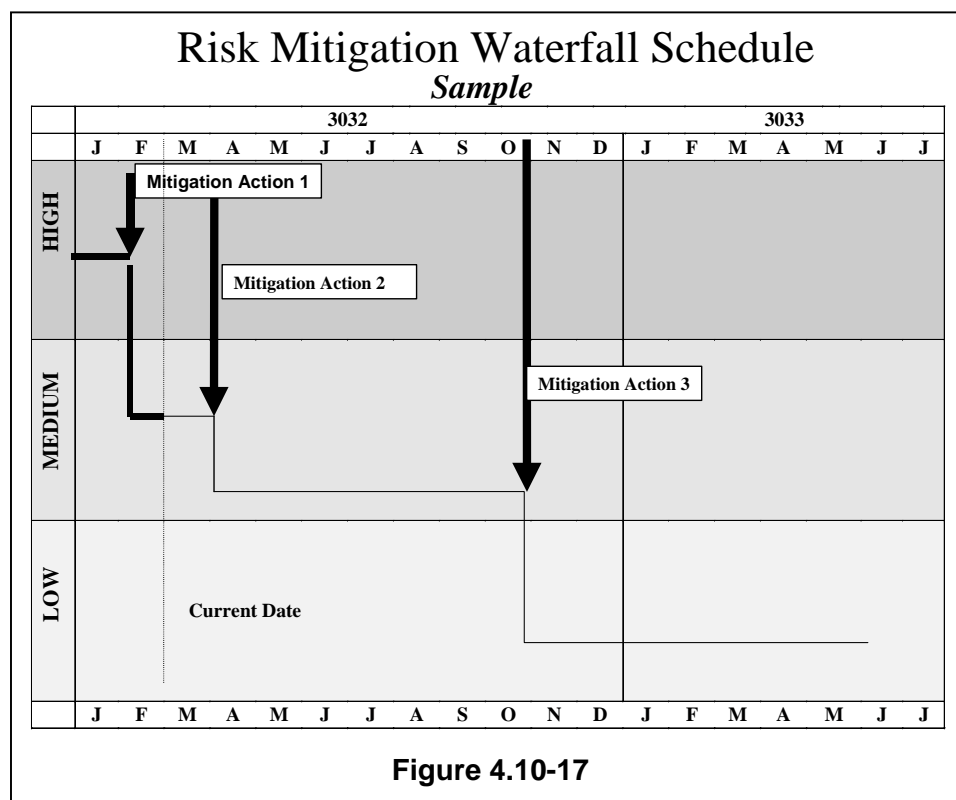# Risk Mitigation Waterfall Schedule
Sample

Figure 4.10-17

438   The risk-mitigation plan becomes the basis for monitoring the success in mitigating each risk.
439   The plan includes, but is not limited to, the following:

440   • A description of the risk for which the plan applies
441

442   • The mitigation approaches, which detail the specific actions that are planned to reduce
443   the risk or eliminate it. It is recommended that these actions be event-based, integrated
444   into a schedule, and have associated with each of them:
445

446   − The decision point or trigger, past or future, that initiates the action or group of
447   actions
448

449   − The resources required to execute the actions (including personnel, capital
450   equipment, facilities, procured equipment)
451

452   − The measures of success to be used for the planned actions or group of actions
453

454   − The fall-back options or contingency plans (if any)
455

456   − The planned completion dates of the actions
457

458   • Risk-mitigation metrics
459

460   • The Risk Worksheet (Figure 4.10-7)
461

462   • The initial Risk Mitigation Plan Summary (Figure 4.10-16)
463

464   • Risk Mitigation Waterfall Schedule (Figure 4.10-17)
465

466   It is recommended that a risk-mitigation plan be evaluated to determine its effectiveness. This
467   analysis is performed in the same manner as initial analysis for the risk. The set of templates
468   used for analysis of the risk may also be used to determine the mitigation in the risk level
469   following the completion of each major action or group of actions. The regular reassessment of
470   the risk and performance to plan using a fixed set of criteria provides a consistent analysis of
471   the impact to the program.

472   The Risk Worksheet (Figure 4.10-7) guides the team through the first three tasks in the Risk
473   Management process: Identify, Analyze, and mitigation planning. When a risk-mitigation plan
474   has been prepared, (Program) Management reviews and approves it based on criteria defined
475   in the Risk Management Plan.

476   **4.10.3.4 Task 4: Implement Risk-Mitigation Plan *(Satisfies iCMM BP 13.05 criteria)***

477   Once risk-mitigation actions are decided, they shall be implemented and carried out effectively
478   so that either risk likelihood or consequence, or both, are reduced to an acceptable level. The
479   implementation of risk-mitigation actions requires that specific tasks be incorporated into the
480   planning, scheduling, budgeting, and cost-accounting systems used on the program.
481   Incorporating risk-mitigation actions directly into the overall program schedule at a point where
482   risk likelihood or consequence may be affected before a risk occurs keeps management and the
483   program team aware of the need to allocate resources (labor, materials, and possibly other

484   resources) to accomplish risk-mitigation tasks. The Risk Mitigation Plan Summary chart (Figure
485   4.10-16) is used as a means of reporting progress in mitigating risks. Each major event in the
486   mitigation plan is identified along with how that event mitigates the risk and to what level.

487   Incorporating the risk-mitigation plans and milestones into these program processes and
488   systems ensures that the risk and its mitigation plans may be monitored and tracked until the
489   risk is eliminated or the risk requires program modification. Risk-mitigation plans may be
490   documented starting with the Risk Worksheet shown in Figure 4.10-7 and a Risk Mitigation
491   Waterfall Schedule shown in Figure 4.10-17. All mitigation activities are shared with and
492   communicated to all stakeholders.

493   **4.10.3.5 Task 5: Monitor and Track Risks** *(Satisfies iCMM PA 14 criteria)*

494   Reassessing currently managed risks is done on a periodic and event basis to reflect current
495   status of the risks as well as to identify and quantify new and emerging risks. New potential
496   risks to the program may be identified at any time. Newly identified risks are analyzed using the
497   same steps described in Section 4.10.3.2.

498   Steps in the risk-tracking process focus on providing the execution teams, interdependent
499   activities, and program management with program risk trends and status. Actual performance
500   of the planned mitigation actions is compared to the expected performance. The bold line on
501   the Risk Mitigation Plan Summary "waterfall area" (see Figure 4.10-17) indicates progress made
502   to date on the mitigation plan. Detailed cost and schedule tracking is done as part of the
503   program schedule and cost-tracking system.

504   It is recommended that the Risk Management plan contain the management visibility
505   requirements for the program. These requirements include reporting frequency and content. A
506   sample of a brief summary of all risks for a particular program (or team) with relatively few risks
507   appears in Figures 4.10-18. A standard reporting format shall be used (see Figure 4.10-19) to
508   facilitate integration of risk information across projects and programs. It is recommended that
509   the risk-management plan also indicate the extent of supporting detail, usually in the format of
510   templates (see Figure 4.10-20).

511   It is recommended that the management visibility effort be focused on monitoring and tracking
512   the effectiveness of the risk-reduction decision. The impact of the risk on program and the
513   relevant **decision** are incorporated into the project schedule as risk-mitigation actions. They
514   are inserted into the program's Integrated Program Schedule (Figure 4.10-21). The lowest-level
515   tasks involved.

Figure 4.10-18

(Extracted from PMR TEMPLATE)

Program Risks Summary

Risk Summary

Total Risks Active on Program	53
Risks with Approved Mitigation Plans	25
New Risks Pending	14

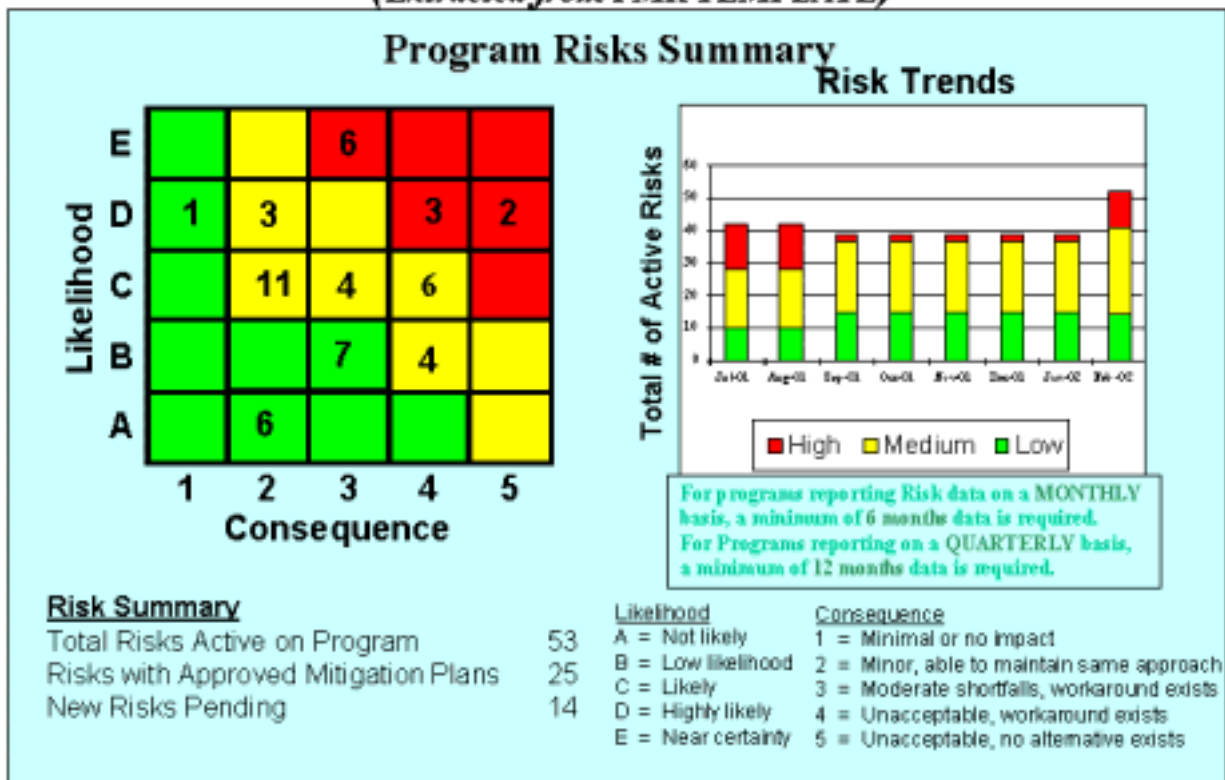| Likelihood		Consequence	
A =	Not likely	1 =	Minimal or no impact
B =	Low likelihood	2 =	Minor, able to maintain same approach
C =	Likely	3 =	Moderate shortfalls, workaround exists
D =	Highly likely	4 =	Unacceptable, workaround exists
E =	Near certainty	5 =	Unacceptable, no alternative exists

Figure 4.10-19

516

(Extracted from PMR TEMPLATES) **Program Risks**

Risk Level	Risk #	Likelihood	Consequence	Risk Type	Risk Item	Mitigation Status	Risk Mitigation Decision Date
H	46	E	4	S	TSO's and AC's may be delayed pending Standards maturity.	PT will work with industry to secure support	Jan-01
H ➤	14	D	5	C	Airspace User Coordination - GA Aircraft users do not accept NEXCOM plan - Benefits for GA not sufficient to engender support - Low end GA Avionics costs too expensive	PT reps will meet with reps of the GA community to determine concerns and strategies for resolution of concerns.	Jun-02
H ▲	30	D	5	C	Business case does not demonstrate ROI for airlines to equip.	PT will establish joint working group with industry to develop business case that industry can support.	Jul-02

List risk updates IN PROGRAM PRIORITY ORDER for each New, High Risk item (Red), and Significant Level Changes (High to Low &/or Low to High).

Likelihood
E = Near certainty
D = Highly likely
C = Likely
B = Low likelihood
A = Not likely

Consequence
1 = Minimal or no impact
2 = Minor, able to maintain same approach
3 = Moderate shortfalls, workaround exists
4 = Unacceptable, workaround exists
5 = Unacceptable, no alternative exists

Risk Level:
H - High   M - Medium   L - Low
➤ = same as last report   ▲ = up from last report
▼ = down from last report

Risk Type
T = Technical
S = Schedule
C = Cost

Note: There is a difference between a risk and an issue. If something is a certainty, it is no longer a risk and should be described as an issue and reported on the issues/concerns slide.

Initially each High risk should be briefed. Subsequently, any new or major change to a risk item should be captured on this slide. See attached proposed "Risk Management" (Attachment #1) for guidance on how to assess and report program risks.

Figure 4.10-20

517
518 are flagged with the assessed risk level; higher-level Work Breakdown Structure tasks inherit
519 the maximum risk level present in any subordinate task. Hence, review of the schedule at any
520 level from

521 **Integrated Program Schedule: summary level (top) and "drill-down" to lowest level tasks (bottom).**

ID	Task Name	Risk	Start	Finish
1	Mission Analysis		10/1/99	10/5/99
7	Investment Analysis		10/6/99	10/11/99
17	Solution Development	●	10/11/99	3/22/07
18	Program management		10/12/99	10/12/55
22	System Engineering	●	10/11/99	1/03/07
23	System Requirements and Definition		10/13/99	10/13/99
25	Analysis, Design, and Integration	●	6/31/01	1/03/07
26	Enhanced Visual Approach - Level 1	●	3/6/02	5/24/03
44	CDTI-Enhanced Flight Rules - Level 2	●	2/28/02	1/7/05
70	CDTI-Enhanced Flight Rules - Level 3	●	10/20/03	1/03/07
96	Terminal Area Multilateration Performance Evaluation	○	12/31/01	1/24/03
113	Terminal Area Common ARTS Integration	●	6/31/01	6/21/04

Risk information displayed at summary task level in the program Integrated Master Schedule (IMS)

● High risk
○ Medium risk
○ Low risk

ID	Task Name	Risk	Start	Finish
1	Mission Analysis		10/1/99	10/5/99
7	Investment Analysis		10/6/99	10/11/99
17	Solution Development	●	10/11/99	3/22/07
18	Program management		10/12/99	10/12/55
22	System Engineering	●	10/11/99	1/03/07
23	System Requirements and Definition		10/13/99	10/13/99
25	Analysis, Design, and Integration	●	6/31/01	1/03/07
26	Enhanced Visual Approach - Level 1	●	3/6/02	5/24/03
27	Resolve concerns with data collection procedures	●	3/6/02	4/17/02
28	Carrier #1 equipage	●	3/20/02	3/20/03
29	Data collection period #1		4/17/02	7/10/02
30	Metrics report #1		7/17/02	7/17/02
31	Data collection period #2		7/17/02	10/9/02
32	Metrics report #2		10/16/02	10/16/02
33	Data collection period #3		10/16/02	1/8/03
34	Metrics report #3		1/15/03	1/15/03
35	Data collection period #4		1/15/03	4/9/03
36	Metrics report #4		4/16/03	4/16/03
37	Document 1% - 3% improvement to terminal arrival rate	○	4/16/03	5/7/03
38	Decision Point - Does data support Level 1 equipage?		6/18/03	6/18/03
39	Certify CDTI use during visual approach	○	6/18/03	5/24/03
44	CDTI-Enhanced Flight Rules - Level 2	●	2/28/02	1/7/05
70	CDTI-Enhanced Flight Rules - Level 3	●	10/20/03	1/03/07
96	Terminal Area Multilateration Performance Evaluation	○	12/31/01	1/24/03
113	Terminal Area Common ARTS Integration	●	6/31/01	6/21/04

"Drill-down" capability - Risk information displayed for lowest level tasks; summary tasks show highest level of risk for any subordinate task

522 **Figure 4.10-21 – Risk Information Incorporated Into Program**

523 summary tasks (Figure 4.10-21, top) to lowest-level tasks (Figure 4.10-21, bottom) allows
524 program management to maintain appropriate risk visibility, and also allows "drill-down" to
525 increasing levels of detail as the schedule view is expanded.

526 Effective program management always involves examining cost and schedule during review of
527 the progress of the program. Making risk information visible as part of the IMS ensures that risk

528   information receives ongoing management attention. Integrating program risk data into the
529   master schedule fosters better, risk-based decisionmaking in at least three ways:

530   (1) The need for separate risk reviews competing for the program manager's time and
531   energy is eliminated.
532

533   (2) Integrating the risk information into the IMS effectively prevents isolation of the risk efforts
534   from the mainstream tasks and program milestones. The risk profile of the program is
535   presented as part of the overall management view of the program. As each decision point is
536   reached, the risk information associated with that event is portrayed, and hence, shall be
537   considered.
538

539   (3) The portrayal of program progress illustrated in Figure 4.10-21 alerts management to
540   when a decision needs to be made and what that decision is. This provides visibility across
541   the entire program *in advance* of impending decision points so that the necessary relevant
542   information is provided in a timely manner to support an informed decision.
543

544   **4.10.4 Outputs** *(Satisfies iCMM Artifacts criteria)*

545   The five major outputs of this process are:

546   • Risk-Mitigation Plans (see Section 4.10.3.3)
547

548   • Risk Mitigation Plan Summary (Figure 4.10-17)
549

550   • Program Risk Mitigation Progress Chart (Figures 4.10-18)
551

552   • Program Risk Summary (Figures 4.10-19 and 4.10-20)
553

554   • Program Risk Register (Figure 4.10-22)
555

556   It is recommended that the Program Risk Summary, the Risk Mitigation Plan Summary, and the
557   Program Risk Mitigation Progress charts be briefed at all regular program reviews.
558   Management decisions are based on the above information. It is recommended that a complete
559   status of a given risk be briefed when the risk is identified and immediately following the risk
560   realization date.

561   It is recommended that the Risk-Mitigation Plan be considered an appendix to the IPP and
562   Acquisition Program Baseline. It shall be handled as an integral part of program effort.

563   **4.10.5 Risk Management Tools**

564   The tools needed to implement this process include:

565   • Approved Risk Management Plan
566

567   • FAA Risk Worksheet
568

569   • Likelihood and consequence templates tailored for the program
570

571   • Risk Mitigation Plan Summary

572

573   • A means to communicate results across a program (electronic mail, servers, etc.)

574

575   • A means to document the results of the process and manage the outputs (databases,
576   spreadsheets, word processors, etc.)

577

578   The risk register (see example in Figure 4.10-22) is a listing of risk information associated with
579   achieving program objectives. If risk registers are created and maintained by each project, a
580   single composite register of all interdependency risk items shall be developed for the program.
581   These registers are to be consistently used to monitor and track overall risk status within team
582   meetings, program management reviews, and major program reviews. Immediately following
583   identification and analysis of a new medium or high risk or when a significant change occurs in a
584   previously identified risk, changes shall be incorporated in the register and other documents and

FAA Program Risk Register

(Example)

DATE 04/15/**3032**
Page __1__ of __1__
Revision

Risk #	Likelihood	Consequence	Risk Level/Change	Risk Item/Consequence	Next Milestone date	Risk Resolution Date	Mitigation Status	Risk Type
1	4	3	M ▼	Sweep rate low/ delays-benefits loss	30320515	30321017	On Track	T
2								
3								

Consequence Key:
1= Minimal impact
2= Minor, able to maintain same approach
3= Moderate shortfalls, workaround exists
4= Unacceptable, workaround exists
5= Unacceptable, no alternative exists

Risk Level:
H - High   **M** - Medium   **L** - Low
▶= same as last report   ▲= up from last report
▼= down from last report

Risk Type:
Ⓣ - Technical
Ⓢ - Schedule
Ⓒ - Cost

Figure 4.10-22

585   the new risk identified to stakeholders. The distribution list is to be established and
586   documented in a program's Risk Management Plan. Computer database systems may be
587   needed to manage these outputs for large programs. Smaller programs may often be able to
588   use desktop computer techniques.

589   At a minimum, the following information shall be included in the risk register:

590   **4.10.5.1.1.1 Risk Register Identification and Creation/Update Date**

591   This is the name of the program risk item. Include the root cause of the risk in this section.

592

593   **4.10.5.1.1.1.1 Risk Identification Number**

594   This number is code that identifies a unique sequence.

595   **4.10.5.1.1.1.2 Likelihood**

596   This is a figure-of-merit indicating the relative likelihood/probability that the identified risk will
597   actually occur (Likelihood Template, Figure 4.10-9).

598   **4.10.5.1.1.1.3 Consequence**

599   This is a figure-of-merit indicating the relative severity of consequences/impacts that could result
600   if the identified risk did occur (Consequences Templates, Figures 4.10-10, 4.10-11, and 4.10-12,
601   for examples).

602   **4.10.5.1.1.1.4 Risk Level/Change**

603   This is a single letter indicating the assessed risk of an item as high, medium, or low (H, M, L)
604   or, red, yellow, or green (R, Y, G), respectively. An arrow that indicates the direction that the
605   risk has moved since the last revision to the risk register demonstrates the risk change.

606   **4.10.5.1.1.1.5 Risk Consequence Description**

607   This is a brief, well-stated description of the risk's negative consequences.

608   **4.10.5.1.1.1.6 Next Milestone Date**

609   This date is the projected date at which the risk level converts to lower risk. This is traceable to
610   the Risk Mitigation Plan Summary (See Figure 4.10-16).

611   **4.10.5.1.1.1.7 Risk Realization Date**

612   This is the date of the event that either makes the risk a real part of the program or eliminates
613   the need to track the risk. Early in the program it may be difficult to predict an exact date but a
614   general timeframe needs to be developed. As the program matures, date realization occurs. It
615   is recommended that these dates be reviewed regularly and be on the program master
616   schedule.

617   **4.10.5.1.1.1.8 Mitigation Status**

618   The currently planned mitigation actions are defined.

619   **4.10.5.1.1.1.9 Risk Type**

620   The risk type designates if the risk is a cost risk, a schedule risk, or a technical risk (see
621   Paragraph 4.10.3.1.1).

622   **4.10.5.1.1.10 Risk-Mitigation Plan Status**

623   The teams regularly update and report the status of the risk-mitigation plan for each risk being
624   tracked that requires risk handling. Actions are initiated as required in which mitigation plan
625   activities are not being accomplished. The risk status is also reviewed with program

626 management on a regular basis. A sample of a brief summary of all risks for a particular
627 program (or team) is shown in a Program Risk Summary (Figures 4.10-18 and 4.10-19) for use
628 depending on program size.

629 An example of a database tools is "Risk Radar" (a tool free to the government that may be used
630 to generate many of the risk work products (see Section 4.10-7).   A version of Risk Radar that
631 incorporates the FAA templates and forms is available for download (http:TBD). This software
632 is available free to all FAA programs (including contractors for use in supporting FAA programs).
633 It requires MS Access 2000 and interfaces with MS Project 2000 for schedule linkage to the
634 overall Program Master schedule.

635 Analytic tools may be used for probabilistic analysis of schedule uncertainty or technical
636 uncertainty. Critical Path Analysis tools may be used with the Integrated Program Schedule to
637 regularly evaluate schedule risk. In a similar fashion, commercial applications (e.g., @RISK)
638 may be applied to technical parameters (such as weight, latency, power, computer throughput)
639 to establish confidence ranges. Results from these probabilistic analyses may support the
640 overall risk analysis task of establishing a likelihood of occurrence. Further details on the use of
641 probabilistic analysis appear in textbooks and technical papers that cover statistical analysis for
642 risk management.

643 **4.10.6 Risk Management Process Metrics *(Satisfies iCMM PA 18 criteria)***

644 It is recommended that Risk Management-related metrics be focused on Program and/or
645 Project success criteria. At the Program level these metrics measure program progress to plan.
646 Earned Value Management is an excellent set of measures to portray the extent of schedule
647 and cost risk in a program. The variance to plan for either Schedule Performance Index or Cost
648 Performance Index may be used as a measure of risk on the Program. Technical or
649 performance risk may be measured through by using Technical Performance Measures. The
650 projected and/or actual variance to performance requirements is a measure of technical risk. At
651 a lower level, metrics for the Risk Management process itself may include:

652 • **Total risks identified over time; total high risks, total medium risks.** The objective
653 is to provide visibility into risk trends over time.
654

655 • **Percent of risks (medium and high) with approved mitigation plans.** The objective
656 is to measure the effectiveness of handling the risks requiring action.
657

658 • **Percent of overdue mitigation activities.** The objective is to measure the
659 effectiveness of meeting mitigation plan schedules.
660

661 • **Aging of active risk records.** The objective is to gain insight into the currency of the
662 risk database.
663

664 • **Number of risks past their realization date.** The objective is to provide an indicator of
665 the effectiveness to handle risks in a timely manner.
666

667 **4.10.7 References**

668 1. AFMC, "Acquisition Risk Management Guide," USAF Pamphlet 63-101.
669

2. ANSI/EIA-632-1998, pp. 11, 13, 14, 17, 30, 33-4, 45, 49, 52, 67, 75, 77, 81, 96, 109, Requirement 24.

3. Blanchard & Fabrycky. "Systems Engineering and Analysis" (3rd ed.). Prentice Hall, 1998, pp. 657-661.

4. Conrow, Edmund H. "Effective Risk Management." American Institute of Aeronautics and Astronautics, Inc., 2000.

5. DoD 4245.7-M. "Transition from Development to Production." Chapter 9-8.

6. DOT H 1350.252. Departmental Guide to Risk Management Planning. May 1999.

7. DSMC. "Risk Management Guide." Available: http://www.dsmc.dsm.mil/pubs/gdbks/risk_management.htm

8. DSMC. "Systems Engineering Management Guide." Chapter 15, 1990.

9. EIA 632, 8/09/02. Rev. 99, Chg.H.

10. FAA AMS Paragraph 2.9.14.

11. FAA Acquisition Program Baseline Template.

12. FAA Orders 1900.47, 1050, 1600, 3900, and 1370.82.

13. FAA-P-1810. "Acquisition and Program Risk Management Guidance." December 1996.

14. FAA Report No. WP-59-FA7N1-97-2. "Risk Assessment Guidelines for the Investment Analysis Process." July 1999.

15. GAO/AIMD (Accounting and Information Management Division)-10.1.13. "Assessing Risks and Returns: A Guide for Evaluating Federal Agencies' IT Investment Decision-making." February 1997.

16. GAO/AIMD-99-139. "Information Security Risk Assessment." August 1999.

17. GAO/OCG-00-12. "Determining Performance and Accountability Challenges and High Risks." August 2000.

18. Grady, Jeffery O. "Requirements Analysis." McGraw-Hill, 1993, p.462-465.

19. Grady, Jeffery O. "System Engineering Planning and Enterprise Identity." CRC Press, 1995, p. 168-177.

20. Grady, Jeffery O. "System Integration." CRC Press, 1994, p. 149.

21. NASA. "NASA Systems Engineering Handbook.," 1995, p. 37-44.

22. OMB Circular No A-11, Part 7 "Planning, Budgeting, Acquisition, and Management of Capital Assets", June 2003

721   23. PMBOK Chapter 11.
722
723   24. Ross, J.F. "Living Dangerously." Perseus Publishing, March 2000.
724
725   25. US Navy Best Practices, NAVSO P-8871